

JTRSY

Public-Contract and Deployment Security Assessment

Janus Henderson Anemoy Treasury Fund
Public-evidence review of current multichain token deployments

REPORT	B3-JTRSY-2026-001
ISSUED	1 October 2026
BASELINE	EVM token/configuration and callback-sample blocks, plus Solana finalized slots, recorded 28-29 September 2026
AUTHOR	bench3.ai

Contents

1 Executive Summary 3

2 Scope and Assessment Basis 4

3 System and Threat Model 4

4 Technical Assessment 5

5 Recorded Validation 7

6 Findings and Control Observations 8

7 RWA Linkage and Public Verifiability 10

8 Limitations and Conclusion 11

A Deployment and Authority Inventory 12

B Evidence and Source Index 13

Assessment of the identified public JTRSY token contracts, restriction configuration and administrative surfaces. Exact observation points, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the public smart-contract and configuration evidence for JTRSY, the Janus Henderson Anemoy Treasury Fund token. The assessed production baseline comprises eight EVM deployments currently listed by Centrifuge—Ethereum, Base, Arbitrum, Avalanche, Plume, BNB Smart Chain, Monad and Pharos—and a separately reviewed Solana Token-2022 mint. [E01-E03; S01]

The eight EVM deployments were active, callable token surfaces at their recorded blocks. Each had a nonzero FullRestrictions hook; read-only token and direct-hook probes completed with the recorded success results, and complete Rely/Deny history replay left only the official Root, Spoke and BalanceSheet wards. The Solana mint was materially different: at finalized slot 451,407,195 it had zero supply, one frozen zero-balance associated token account and no official Solana vault or issuance/redemption program identified. [E01-E03]

Assessment conclusion

No reportable implementation vulnerability was confirmed in the examined EVM restriction and ward paths or in the observed Solana token configuration. Three control observations are reported. The result is bounded to the recorded deployments and states; it does not establish the security of an unobserved future Solana issuance lifecycle or the completed retirement of X Layer.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; privileged governance, dormant-deployment control and legal/accounting boundaries
Unresolved technical issues	No ordinary-caller defect was established; the remaining gaps concern deployment lifecycle, inactive Solana behavior and private controls

Material qualifications

The current public deployment table no longer lists X Layer, although the retained registry records JTRSY code at 0xc18e6f730896971a79d748e8dea61067a9bc6040 at X Layer block 71,765,200. No authoritative retirement, migration-completion or residual-asset record was obtained. This report therefore treats X Layer as offboarded from the current manifest but with unresolved lifecycle status, not as a current assessed production network and not as proven safely decommissioned. [E01, E04; L01]

Solana's zero supply materially limits current economic exposure, but it also means production issuance, redemption, cross-chain and end-to-end supply-accounting behavior could not be observed. Its threshold-two Squads controller has no on-chain timelock, and private member custody and approval procedures were not assessed. [E02-E03; O02; L02-L03]

2 Scope and Assessment Basis

2.1 Assessment identity

Parameter	Assessment basis
Assessment type	Public-evidence deployed-contract, configuration and source-correspondence assessment
Current EVM scope	Ethereum, Base, Arbitrum, Avalanche, Plume, BNB Smart Chain, Monad and Pharos
Solana scope	Token-2022 mint, shared program dependency and authority/configuration state at finalized slots 451,407,195 and 451,408,537
Historical/offboarded scope	X Layer identifier retained for lifecycle disclosure only; absent from the current official table
Evidence cutoff	30 September 2026; latest technical observations were recorded on 29 September 2026

2.2 Included work

For the eight current EVM deployments, the retained assessment reconstructed token and hook identities, read live hook configuration at fixed blocks, exercised read-only restriction and callback probes, replayed complete Rely/Deny histories, classified surviving wards against the official Centrifuge deployment manifest and reviewed the release-tag FullRestrictions behavior relevant to ordinary transfers, cross-chain classification and restriction updates. [E01; S01-S05]

For Solana, the retained assessment read the Token-2022 mint and account state, enumerated token accounts, reconstructed mint/freeze/permanent-delegate and metadata authorities, derived the Squads vault PDA, decoded the multisig threshold, timelock and member-permission entries, recorded the zero-supply state, and identified the shared Token-2022 ProgramData, upgrade authority, executable hash and public verification commit. No production transaction was signed or broadcast. [E02-E03; S11]

2.3 Exclusions

Excluded are private investor onboarding and transfer-agent records, fund-administration and custody systems, order acceptance, NAV calculation and publication controls, banking and cash settlement, key custody, internal approvals, incident response, and any unlisted backend or future Solana application program. The broader Centrifuge protocol was not audited as a standalone system; only components material to the identified JTRSY token paths were considered. [L02-L05]

The public deployment manifest and archived registry establish listed deployment identities and attribution; they do not by themselves prove that every deployment was fully audited. Conclusions are tied to the exact fixed blocks and slots in Appendix A. [E01-E04]

3 System and Threat Model

JTRSY represents a fund share across multiple ledgers. On the current EVM networks, Centrifuge token contracts apply an external FullRestrictions hook to transfers and expose ward-authenticated administration. Root, Spoke and BalanceSheet contracts form the recorded privileged control set. On Solana, Token-2022 enforces mint and account semantics while a Squads vault PDA holds the principal issuer authorities. These are separate execution models and were assessed separately. [E01-E03]

Layer	Security-relevant state	Boundary in this assessment
EVM holder and allowance spender	Balances, allowances and ordinary transfer requests	Cannot update restriction data or token configuration without an authenticated ward/manager path.
EVM ShareToken / Tranche	Balances, supply, hook address, hook data and ward authorization	Current token and hook configuration reviewed at eight fixed blocks.
EVM Root, Spoke and BalanceSheet	Surviving privileged wards and protocol-mediated issuance/accounting operations	Address identity and complete ward history reviewed; private approval and key controls excluded.
Solana Token-2022 mint	Supply, mint/freeze/permanent-delegate powers, default-frozen accounts and metadata	Configuration reviewed while supply was zero; no active issuance/redemption lifecycle existed to observe.
Squads controller	Threshold approvals and vault-PDA execution of Token-2022 authority	PDA derivation and on-chain settings reviewed; member identity and custody excluded.
Fund and legal records	Transfer-agent register, NAV, portfolio, custody and settlement	Public linkage assessed; no legal, reserve or financial attestation provided.

3.1 Security objectives

The threat model includes ordinary external addresses, token holders and allowance spenders without privileged Centrifuge or Squads authority. The principal objectives were to preserve restriction enforcement, prevent unauthorized mutation of eligibility state or hook configuration, prevent ordinary transfers from inducing nested privileged state changes, constrain administrative authority to the documented controller set, and preserve clear ledger boundaries between current and dormant deployments.

Compromise, collusion or erroneous use of legitimate wards or Squads members remains a material trust dependency. Authorized power is reported as a control observation unless the evidence establishes a violated implementation invariant.

4 Technical Assessment

4.1 Current EVM deployment identity and transfer hooks

The current official manifest listed eight EVM deployments. Ethereum, Base, Arbitrum, Avalanche, Plume and BNB returned hook 0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC; Monad and Pharos returned 0x8E680873b4C77e6088b4Ba0aBD59d100c3D224a4. The two runtime families were nonempty and had the fixed hashes recorded in Appendix A. [E01; S01]

At each token/configuration snapshot block, token-level detectTransferRestriction(0,0,0) returned the recorded value 1. Direct calls to the configured hook with an allowed redemption-shaped zero-value tuple returned true from checkERC20Transfer and 0x3f71910e from onERC20Transfer. The callback samples used later blocks on Ethereum (26,077,655 versus token snapshot 26,077,429), Arbitrum (509,785,074 versus 509,774,491) and BNB Smart Chain (124,570,349 versus 124,564,347); the other five callback samples used the same blocks as their token snapshots. These read-only samples establish compatible callable code for the sampled path at their stated observation blocks; they do not constitute comprehensive transfer-state testing. [E01]

4.2 Restriction update and callback behavior

The recorded review of the official release-tag BaseTransferHook and FullRestrictions sources found that onERC20Transfer evaluates the restriction predicate and returns the expected selector, while onERC20AuthTransfer is pure. Restriction-management functions update account hook data but expose no ordinary-caller route to replace the token's hook. The callback does not transfer tokens, call token-administration functions or mutate hook data during an ordinary transfer. [E01; S03-S04]

FullRestrictions is holder/recipient based. It blocks the relevant frozen source or destination condition and applies membership predicates appropriate to deposits, redemptions, ordinary transfers and cross-chain execution. transferFrom still requires the holder's allowance. The official access-permission documentation did not impose an independent membership requirement on a non-custodial allowance operator, so the absence of the spender from the hook predicate did not establish a policy bypass. [E01; S04-S05]

4.3 Ward history and privileged configuration

The recorded assessment replayed every Rely and Deny event from deployment through the fixed snapshot for all eight EVM tokens. Exactly three current wards remained on each chain: the official Root, Spoke and BalanceSheet addresses for that network group. No deployer, migration-only address or unidentified ward survived in the replayed set. [E01; S01-S02]

This supports the current controller inventory but does not remove the trust dependency. An authorized ward can invoke privileged token operations and change relevant configuration. A later rely, deny or file("hook", ...) action can change the result without changing the token address. [O01]

4.4 Solana zero-supply deployment

At finalized slot 451,407,195, mint JTRu97Z4oduVwfVBWdf1fSAz8h7CBBPqEo4Jco9fZPj had six decimals and raw supply zero. The account enumeration found one associated token account, which was frozen and held zero units. The mint exposed permanent-delegate, default-account-state, metadata-pointer and token-metadata extensions; no transfer hook, transfer fee, confidential-transfer or pausable extension was present. [E02-E03]

Mint, freeze, permanent-delegate and metadata-update authority were held by vault PDA 3JiU6sJt94WcD6r7EFTUnJo6By9DJ9WJxovRGfY9oseb, derived as vault index 0 of Squads multisig F8uKD1uQ4o2NVizM8VfNvBMNoL18WXXbhTjKqfzvBTSX. The multisig threshold was two, the timelock was zero, and six of eight member entries had the full permission mask. The Squads program was frozen, but no accepted exact source/build mapping for that mainnet binary was established. [E02-E03; O02]

The frozen Squads deployment does not make the complete Solana execution path immutable. The mint also depends on the shared upgradeable Token-2022 program, whose recorded deployment, authority, executable hash and public verification commit are listed in Appendix A. This is a shared platform trust dependency, distinct from the issuer's Squads threshold and from the unresolved Squads source/build correspondence. No ordinary-caller path to exercise either authority was established. [E02-E03; S11; O02]

Metadata-update authority had moved to the Squads vault, while bootstrap address Eg37TXi7ojfPT4kQPFUu6umtvz3cCN2Xif5TgQKDd68C retained metadata-pointer authority. That separate role can affect where interfaces obtain metadata; it does not by itself confer mint, freeze or transfer authority. [E02-E03]

4.5 Network lifecycle distinction

The 29 September 2026 current official table listed the eight EVM deployments above plus the Solana mint. It omitted X Layer. The retained earlier registry nevertheless contains X Layer ShareToken code at 0xc18e6f730896971a79d748e8dea61067a9bc6040 and block 71,765,200. The report therefore separates: current EVM scope; current-listed but dormant Solana scope; and an offboarded-from-manifest X Layer identifier whose retirement state was not proven. [E01-E04; L01]

5 Recorded Validation

The table summarizes the fixed-height reads, event reconstruction and configuration checks preserved in the assessment evidence. These observations are narrower than a comprehensive regression or property-test suite. [E01-E03]

ID	Recorded check	Outcome and evidentiary limit
V01	Read hook() and hook runtime on each current EVM deployment	All eight hooks were nonzero and contained code at the fixed blocks; later privileged replacement remains possible.
V02	Token-level restriction probe	detectTransferRestriction(0,0,0) returned the recorded value 1 on all eight chains; this is a narrow read-only input, not broad transfer coverage.
V03	Direct hook success-path probes	checkERC20Transfer returned true and onERC20Transfer returned 0x3f71910e for the sampled allowed tuple on all eight chains. Ethereum, Arbitrum and BNB samples used later callback blocks than their token/configuration snapshots; the other five used the same block.
V04	Complete Rely/Deny history replay	Exactly Root, Spoke and BalanceSheet survived per current EVM chain; current wards were derived from complete event replay.
V05	Solana mint and token-account enumeration	Supply and the sole enumerated token-account balance both equaled zero at the fixed slot; no active lifecycle was exercised.
V06	Squads PDA and control decode	Vault index 0 derivation, threshold two, zero timelock and member permission entries were recorded; private member custody was not assessed.
V07	Final Solana recheck	At finalized slot 451,408,537 the mint remained owned by Token-2022 and the Squads program remained executable.

No production transaction was signed or broadcast, no privileged identity was impersonated and no local validator or simulator was used for the recorded Solana review. The EVM checks were fixed-height reads and event-history reconstruction. [E01-E03]

6 Findings and Control Observations

No implementation vulnerability was confirmed. The observations below identify material trust, governance and integration boundaries and are not included in vulnerability severity totals. No issuer response or remediation verification was supplied.

ID	Title	Category / status
B3-JTRSY-O01	EVM restriction and token administration remains privileged	Privileged-control observation; applicable at snapshot
B3-JTRSY-O02	Dormant Solana execution retains issuer-governance and shared program-upgrade dependencies	Governance/deployment-maturity observation; applicable at snapshot
B3-JTRSY-O03	Public token balances do not close the legal-share and custody ledger	RWA integration observation; applicable to disclosed model

001 | EVM restriction and token administration remains privileged

Attribute	Record
Affected components	Current EVM ShareToken/Tranche deployments, FullRestrictions hooks, Root, Spoke and BalanceSheet wards
Classification	Control observation. No implementation-vulnerability severity assigned.
Evidence	E01; S01-S05

Description. Complete event replay identified only the official Root, Spoke and BalanceSheet as surviving wards on each current EVM deployment, and every observed hook was nonzero and callable. These positive configuration results remain subject to legitimate privileged change: authorized controllers can invoke administrative operations and can change the hook or ward set through the supported governance paths.

Impact and preconditions. Compromise, collusion or erroneous authorized operation could alter eligibility enforcement, token administration or accounting behavior. The risk requires valid privileged authority; no ordinary-caller escalation to those powers was established. Private signer custody, approval separation and incident-response controls were not assessed.

Recommendation. The issuer and Centrifuge operators should maintain a signed, chain-specific manifest of token, hook and expected ward identities; enforce multi-party change approval; monitor Rely, Deny and hook File events; and reconcile every change against the approved manifest before resuming issuance or transfers after an administrative update.

Status. Applicable at the assessed blocks; organizational mitigations not independently verified.

O02 | Dormant Solana execution retains issuer-governance and shared program-upgrade dependencies

Attribute	Record
Affected components	Solana mint JTRu97Z4oduVwfVBWdf1fSAz8h7CBBPqEo4Jco9fZPj; Squads vault and multisig; metadata-pointer authority; shared Token-2022 program dependency
Classification	Governance and dormant-deployment control observation. No implementation-vulnerability severity assigned.
Evidence	E02-E03

Description. The Squads vault controls mint, freeze, permanent-delegate and metadata-update authority with a threshold of two and no timelock. Six of eight recorded member entries had full permissions. A separate bootstrap address retained metadata-pointer authority. Although the Squads program was frozen, the mint also depends on the shared upgradeable Token-2022 program identified in Appendix A. The supply was zero, so these powers did not govern circulating investor units at the snapshot; they would become material if issuance begins.

Impact and preconditions. Two qualifying Squads approvals can authorize minting, freezing or permanent-delegate actions without an on-chain delay. Metadata-pointer authority can change interface-facing metadata location, and authorized use or compromise of the shared Token-2022 upgrade authority could change token-program execution semantics. These conditions require control of the relevant privileged authority; no route for an ordinary external account to sign as the vault PDA or exercise the Token-2022 upgrade authority was established.

Recommendation. Before activating Solana issuance, the issuer should document member independence and custody, increase the approval threshold where compatible with recovery requirements, introduce an operational delay for routine high-impact actions, separate metadata control where practical, publish the exact issuance/redemption program and build identity, and monitor Squads, Token-2022 loader/verification state, authority changes and permanent-delegate actions.

Status. Applicable to the dormant zero-supply deployment; future production controls not verified.

O03 | Public token balances do not close the legal-share and custody ledger

Attribute	Record
Affected components	All JTRSY ledgers; transfer-agent register, fund NAV, portfolio and custody records
Classification	RWA integration/control observation; not a demonstrated contract defect
Evidence	E05; S07-S10

Description. Public materials describe JTRSY tokens as preliminary evidence of ownership in a BVI Professional Fund and describe Centrifuge hub-and-spoke accounting, NAV and share-price publication. The public record does not expose a synchronized holder-level transfer-agent register, itemized custodian assets or a same-cutoff reconciliation of all legal shares across chains.

Impact and preconditions. An integrator that treats an on-chain balance, a single-chain supply or a published NAV as complete proof of legal ownership and underlying custody may overstate settlement finality or backing. No token-contract accounting defect was demonstrated by this limitation.

Recommendation. Fund operators and integrators should reconcile token supply, the authoritative transfer-agent register and fund/custody records at aligned cutoff times, identify the legally authoritative record for discrepancies, and expose lifecycle status for each supported or retired network. User interfaces should distinguish indicative on-chain state from finalized legal ownership and settlement.

Status. Applicable to the disclosed product model; private register and custody reconciliation not assessed.

Classification criteria

Where a vulnerability is established, severity reflects supported impact, realistic preconditions and reachability. Control observations identify material trust or operational dependencies without establishing an implementation defect. Scope limitations identify claims the available evidence cannot support. Observations and limitations are excluded from vulnerability totals.

7 RWA Linkage and Public Verifiability

JTRSY is described as a direct share in a BVI Professional Fund. Public materials state that the token is preliminary evidence of share ownership and that the fund invests primarily in short-duration government debt through the disclosed structure. Centrifuge's hub-and-spoke system provides multichain issuance/accounting and publishes share-price information. [E05; S07-S10]

Assertion	Available public evidence	Assurance boundary
Product identity	Anemoy and Janus Henderson materials identify the fund and Centrifuge deployment relationship. [S07, S10]	Supports product identity; not a legal opinion on holder rights.
Current network identity	Centrifuge's 29 September manifest lists eight EVM deployments and the Solana mint. [S01, S06]	X Layer is absent from the current list, but completed retirement was not established.
Token execution and restrictions	Fixed-height EVM hook/ward observations and a fixed-slot Solana configuration record. [E01-E03]	Point-in-time public-contract assurance only; private operations excluded.
Fund accounting and price	Public fund and Centrifuge accounting pages describe NAV/share-price and hub-and-spoke accounting. [S07-S09]	No same-cutoff independent reconciliation to the transfer-agent register and custody assets.
Legal ownership and custody	Public product materials describe the fund-share relationship. [S07-S10]	Holder-level register, itemized custody and full legal-share totals were not publicly closed.

The public evidence supports the stated product and accounting linkage, but not a real-time, independently reconciled chain from every token unit to the legal register and underlying portfolio. This report therefore does not assign a reserve-coverage percentage and does not equate a token balance or published share price with completed legal settlement or a custody attestation.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	X Layer is absent from the current official deployment table, but an older retained registry contains the token runtime and no authoritative retirement record was obtained.	X Layer is excluded from the current production opinion; the report does not assert that it was safely decommissioned or that no residual supply, permissions or integration remains.
L02	The Solana mint had zero supply and no official vault, issuance, redemption or bridge program was identified.	Future mint/burn, account-constraint, replay and end-to-end supply-accounting behavior is untested and outside the present conclusion.
L03	Private ward and Squads member custody, approval procedures, monitoring and incident response were unavailable.	The report verifies on-chain controller identities and settings, not organizational effectiveness or resistance to key compromise/collusion.
L04	Transfer-agent, fund-administration, NAV, portfolio, custody and settlement records were not independently reconciled.	No legal-share, financial-statement, reserve, solvency or completed-settlement assurance is provided.
L05	Validation was targeted, public and read-only rather than a complete source audit, property-test campaign or privileged end-to-end exercise.	The absence of a confirmed issue in the examined paths does not establish that every behavior, state transition or future version is defect-free.

Conclusion

The retained source analysis, fixed-height configuration reads and complete ward-history replay support the stated restriction and controller conclusions for the eight current EVM deployments. The recorded Solana review supports the stated zero-supply configuration and Squads authority model. No reportable implementation vulnerability was confirmed in these examined paths.

The opinion is intentionally asymmetric: it addresses active current EVM deployments, a current-listed but dormant Solana mint, and an X Layer deployment omitted from the current manifest whose retirement remains unresolved. Material changes to token code, hooks, wards, Squads settings, authorities, network support or issuance state require reassessment.

This public-evidence assessment was not commissioned by the issuer. It does not guarantee the absence of undiscovered vulnerabilities and does not constitute a financial audit, reserve attestation, legal opinion, regulatory-compliance opinion or investment recommendation.

A Deployment and Authority Inventory

Current EVM deployments

Network / token block / callback block	Token	Configured hook
Ethereum token 26,077,429 callback 26,077,655	0x8c213ee79581ff4984583c6a801e5263418c4b86	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
Base token/callback 51,913,488	0x8c213ee79581ff4984583c6a801e5263418c4b86	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
Arbitrum token 509,774,491 callback 509,785,074	0x8c213ee79581ff4984583c6a801e5263418c4b86	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
Avalanche token/callback 96,337,265	0xa5d465251fbcc907f5dd6bb2145488dfc6a2627b	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
Plume token/callback 96,102,889	0xa5d465251fbcc907f5dd6bb2145488dfc6a2627b	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
BNB Smart Chain token 124,564,347 callback 124,570,349	0xa5d465251fbcc907f5dd6bb2145488dfc6a2627b	0x21Cdcc686fECd9Fb0d3ee300E555C06497B55EcC
Monad token/callback 108,810,117	0xc18e6f730896971a79d748e8dea61067a9bc6040	0x8E680873b4C77e6088b4Ba0aBD59d100c3D224a4
Pharos token/callback 18,831,132	0xc18e6f730896971a79d748e8dea61067a9bc6040	0x8E680873b4C77e6088b4Ba0aBD59d100c3D224a4

The first hook family had runtime Keccak-256 0x7d78de7692e4c7cc9958e2e796c2bbb75cd1bd567fddd03a59488c831c446204; the Monad/Pharos family had runtime Keccak-256 0x107cd5449c9b468640c68f87f2d0146e74e8a5d9b25abd8107061ace3ca168f1. The retained independent reads reported 7,760 runtime bytes for both families. [E01]

EVM ward groups

Networks	Root	Spoke / BalanceSheet
Ethereum, Base, Arbitrum, Avalanche, Plume, BNB	0x7Ed48C31f2fdC40d37407cBaBf0870B2b688368f	0xEC3582fcDc34078a4B7a8c75a5a3AE46f48525aB 0x12a110cE5f0FC871cC72Bc7ECaF35cf39DD0f43e
Monad, Pharos	0xdc9456e7e20f15029C8231Ec433a20F404b7235E	0xEC3582fcDc34078a4B7a8c75a5a3AE46f48525aB 0x12a110cE5f0FC871cC72Bc7ECaF35cf39DD0f43e

Solana deployment

Component	Identifier / state
JTRSY Token-2022 mint	JTRu97Z4oduVwfVBWdf1fSAz8h7CBBPqEo4Jco9fZPj 6 decimals supply 0 at slot 451,407,195
Mint/freeze/permanent-delegate vault	3JiU6sJt94WcD6r7EFTUnJo6By9DJ9WJxovRGfY9oseb
Squads multisig	F8uKD1uQ4o2NVizM8VfNvBMNoL18WXXbhTjKqfzvBTSX vault index 0 threshold 2 timelock 0
Squads v4 program	SQDS4ep65T869zMMBKyuUq6aD6EgTu8psMjkvj52pCf ProgramData Fy3YMJCvwbAXUgUM5b91ucUVA3jYzwWLHL3MwBqKsh8n upgrade authority null
Shared Token-2022 program	TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb ProgramData DoU57AYuPFu2QU514RktNPG22QhApEjnKxnBcu4BHDTY deploy slot 427,147,035 upgrade authority AeLmXCbPaQHGWRLr2saFsEVfmMNUKnXRabWCT9P5twgz executable SHA-256 7ea94a027005b39196fa08e6d0ddcd55ec32eb43266179921a834a1ba2eb1947 verified commit 9bc02757f600ffe754746708a8a072bcd49d1260
Metadata-pointer authority	Eg37TXi7ojfPT4kQPFUu6umtvz3cCN2Xif5TgQKDd68C

Historical/offboarded-from-manifest identifier

X Layer ShareToken: 0xc18e6f730896971a79d748e8dea61067a9bc6040 at retained registry block 71,765,200; runtime Keccak-256 0xc583d36342a6350a5e5bd3c2d9f0b596f7f4f0a1794a784f2f48a2afcbe5bde8. The address is omitted from the current official JTRSY table. Retirement and residual state were not established. [E01, E04; L01]

B Evidence and Source Index

Assessment workpapers are retained separately and are not attached. The scope manifest identifies each record by SHA-256 and includes deployment and source references. Checksums identify records; they do not attest to their contents.

ID	Assessment record
E01	JTRSY EVM deployment, hook and authority assessment
E02	JTRSY Solana deployment and authority assessment
E03	JTRSY Solana deployment state record
E04	JTRSY deployment registry snapshot
E05	Tokenized Treasury RWA anchor and public-verifiability assessment
E06	Tokenized Treasury asset-scope and limitation summary

Primary public sources

- S01** | Centrifuge protocol deployments
Observed 29 September 2026; current JTRSY network and controller manifest.
- S02** | Centrifuge production environment manifests
Public controller-address manifests used to classify replayed EVM wards.

S03 | Centrifuge Protocol v3.1.0 BaseTransferHook

Release-tag source used by the retained review for callback and authenticated restriction-update behavior.

S04 | Centrifuge Protocol v3.1.0 FullRestrictions

Release-tag source used by the retained review for frozen-account and membership predicates.

S05 | Centrifuge access permissions

Official holder and recipient eligibility model observed 29 September 2026.

S06 | Centrifuge documentation deployment commit

Pinned official source identifying the JTRSY Solana mint and current network table.

S07 | Anemoy JTRSY fund page

Public product and legal-linkage description retained in the RWA assessment.

S08 | Centrifuge JTRSY pool page

Public pool and share-price information retained in the RWA assessment.

S09 | Centrifuge on-chain accounting

Official hub-and-spoke accounting description retained in the RWA assessment.

S10 | Janus Henderson partnership announcement

Issuer/manager attribution and fund-strategy context retained in the RWA assessment.

S11 | Solana Token-2022 deployment verification status

Public verification record retained for the Solana assessment; exact correspondence reported to token-2022 commit 9bc02757f600ffe754746708a8a072bcd49d1260.

Scope attachment

jtrsy-scope-manifest-en.json

SHA-256: 742f8dd2d7905fa721e68112719560b9d6c438111a5a73b771a2c1089a42180c